The Department of Defense *Information Assurance* Strategic Plan

V1.1 January, 2004

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Department of Defense Information Assurance Strategic Plan V1.1	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **The Department of Defense,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**20**	

DoD's Information Assurance Strategic Plan Framework

VISION

Dynamic Information Assurance
for the Global Information Grid (GIG)

GOALS and OBJECTIVES

Protect Information to safeguard data (as information) as it is being created, used, modified, stored, moved, and destroyed, at the client, within the enclave, at the enclave boundary, and within the computing environment, to ensure that all information has a level of trust commensurate with mission needs by…

- **Developing and promulgating the GIG IA Architecture**
- **Developing and implementing protection criteria for effective Net-Centric Operations**
- **Developing and deploying protection capabilities across the enterprise**
- **Transforming the Security Management Infrastructure (SMI) to satisfy the agility demands of the end-state GIG**

Defend Systems and Networks by recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies, ensuring that no access is uncontrolled and all systems and networks are capable of self-defense by…

- **Establishing the GiG Network Defense architecture and to-be baseline roadmap to respond to known and advanced threats**
- **Developing and enforcing CND policies across the enterprise to achieve an optimal readiness posture against the outsider "nation state" attacker as well as the threat posed by the insider**
- **Evaluating and deploying CND tools and capabilities in a coordinated manner to achieve required operational capability**
- **Establishing mechanisms and procedures within CND response action guidelines that effectively utilize developed CND tools and capabilities to react and respond to events**
- **Mitigate the Insider Threat across DoD through the implementation of advanced tools, processes, and operational capabilities**

No. 1

Provide Integrated IA Situational Awareness / IA Command and Control (C2) integrating the IA posture into a User-Defined Operational Picture (UDOP) synchronized with NETOPS and emerging Joint C2 Common Operating Picture (COP) programs to provide decision makers and network operators at all command levels the tools for conducting IA/CND operations in Net-Centric Warfare (NCW) by…

- **Developing and deploying an Enterprise Sensor Grid**
- **Establishing effective Indications and Warning (I&W) of potential or ongoing attacks against the enterprise**
- **Developing and deploying an IA User-Defined Operational Picture (UDOP) integrated with evolving NETOPS and Joint C2 COP capabilities**
- **Conducting near-real-time and integrated IA and Network Operations (NETOPS) decision-making across the enterprise**
- **Harmonizing NETOPS, Information Operations (IO), Computer Network Attack (CNA), and Computer Network Defense (CND) policies, doctrine, relationships and operations**

Transform and Enable IA Capabilities innovatively by discovering emerging technologies, experimentation, and refining the development, delivery and deployment processes to improve cycle time, reduce risk exposure and increase return on investments by…

- **Ensuring that IA is integrated and sustained throughout the lifecycle of all DoD programs**
- **Improving the quality of strategic decision making and net-centric IA governance**
- **Expediting the development and delivery of dynamic IA capabilities through innovation**
- **Enabling efficient information sharing and collaboration across traditional boundaries**

Create an IA Empowered Workforce that is well equipped to support the changing demands of the IA/IT enterprise by…

- **Establishing baseline certifications across the enterprise**
- **Continuously enhancing IA skills to keep current with technologies and threats**
- **Providing trained/skilled people when and where needed**
- **Infusing IA awareness and concepts into other disciplines and entities**

We are proud to present the Department of Defense's (DoD's) Information Assurance (IA) Strategic Plan, an update to the Strategic Plan we introduced last year.

Our first Strategic Plan, which was published in October 2003, was a major accomplishment and provided a solid foundation and framework for how we will assure the Department's information. The Vision and Goals in our Strategic Plan are enduring and serve to define a consistent strategic direction to assuring our information. As we stated last year, the Strategic Plan is a living document and we are committed to updating the Plan to ensure our efforts remain a vital and accurate reflection of the major issues facing the Department. We have aligned our investments and strategic initiatives to our Goals and are continuing to define and track milestones and performance measures to gauge their success.

While the overall framework and basic tenets of the Strategic Plan are still valid, we are placing a greater emphasis on a number of areas to reflect the strategic priorities of the Department:

- We have refined the mission statement to reflect the critical role of IA in the Net-Centric Warfare (NCW) mission and to address the priorities of the Assistant Secretary of Defense for Networks and Information Integration (NII).
- We have refined strategic and performance objectives for Goals #1, 2 and 3 to provide a strategic focus on Net-centric transformation and the need for an enterprise IA architecture and policy. Additional emphasis has been placed on the implementation and deployment of key capabilities such as Public Key Infrastructure (PKI), biometrics and the transforma tion of the Security Management Infrastructure (SMI).
- We have refined strategic and performance objectives for Goal #4 to provide a stronger emphasis on full lifecycle integra tion for IA throughout the acquisition process and increased accountability through program management and perform ance measurement. Added emphasis has also been placed on eliminating stove-pipe and redundant processes; realizing the benefits of collaboration across the Community; and leveraging innovation to transform IA technologies and processes.

No. 2 In sharing a draft of this updated Plan with representatives from the Combatant Commands, Services and Agencies, we sought to make sure that it reflects the needs of the Department. The IA Community has a critical role in DoD's transformation to net-work and data centric operations and warfare. This updated Strategic Plan will help to ensure we succeed in that role.

Priscilla Guthrie
Co-Chair, IA Senior Leadership Group

Carol Haave
Co-Chair, IA Senior Leadership Group

Members of the IA Senior Leadership Group:

LTG Steven Boutelle, USA
Army CIO/G-6

Ms. Debra M. Filippi
U.S. Marine Corps

Mr. John Gilligan
U.S. Air Force

Mr. David Wennergren
U.S. Navy

BrigGen Bradley Butler, USAF
U.S. Air Force

BrigGen Ronnie Hawkins, USAF
U.S. Air Force

BG(P) Dennis Moran, USA
U.S. Army

Col David Warner, USAF
U.S. Joint Forces Command

Mr. George Wauer
OSD(DOT&E)

Dr. Andre Van Tilborg
ODUSD AT&L(S&T)

Mr. Robert Carey
Deputy DON CIO

RADM Thomas E. Zelibor, USN
Chief of Naval Operations (N61)

Mr. Richard Hale
Defense Information Systems Agency

Mr. Mike Fleming
National Security Agency

Mr. Mario Balakgie
Defense Intelligence Agency

MG James Bryan, USA
U.S. Strategic Command

Mr. William Dawson
Intelligence Community

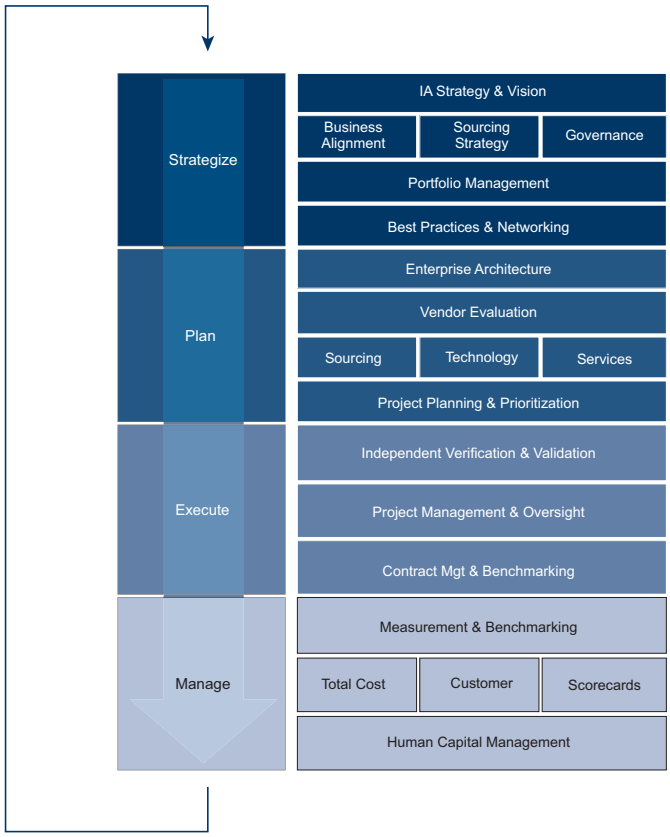
Mr. Robert Lentz
OASD(NII)

MajGen Charles Croom, USAF
AF/XI-2

RADM Nancy E. Brown, USN
The Joint Staff (J6)

MG Emile P. Bataille, USA
U.S. Strategic Command

The Ongoing Lifecycle of IA



The IA Strategic Plan is a living document and we will continue to review our vision, goals and objectives for relevancy, currency , and applicability to keep pace with our changing environment and address significant challenges we face.

We are implementing an ongoing strategic management process to enable the IA Community to implement and manage strategic decisions, respond dynamically to changing conditions, and evolve the strategy as the situation dictates.

Our ability to successfully achieve the Goals in this plan requires the continued commitment and mandate from Senior Leadership and the cooperative support of all members of the IA Community. The most important test of our success in implementation of this Plan is the degree to which people integrate the strategy into their everyday decisions.

Mission

Assure the Department's Information, Information Systems and Information Infrastructure and Support the Department's Transformation to Network and Data-Centric Operations and Warfare

Vision

Dynamic Information Assurance for the Global Information Grid (GIG)

Achieving this vision requires transforming our operations, technologies, processes, and people:

Our Operations

- Warfighters and supporting personnel have confidence in the information needed to achieve Mission Readiness
- Decision makers share a seamless, enterprise-wide, and common view of information, networks, and systems, allowing them to jointly make decisions
- DoD's extended secure enterprise architecture allows sharing of information and knowledge throughout the GIG and enable multi-level information sharing across multiple security domains
- Industry, Allies and Coalition partners are integrated, as appropriate, into daily operations

Our Technologies

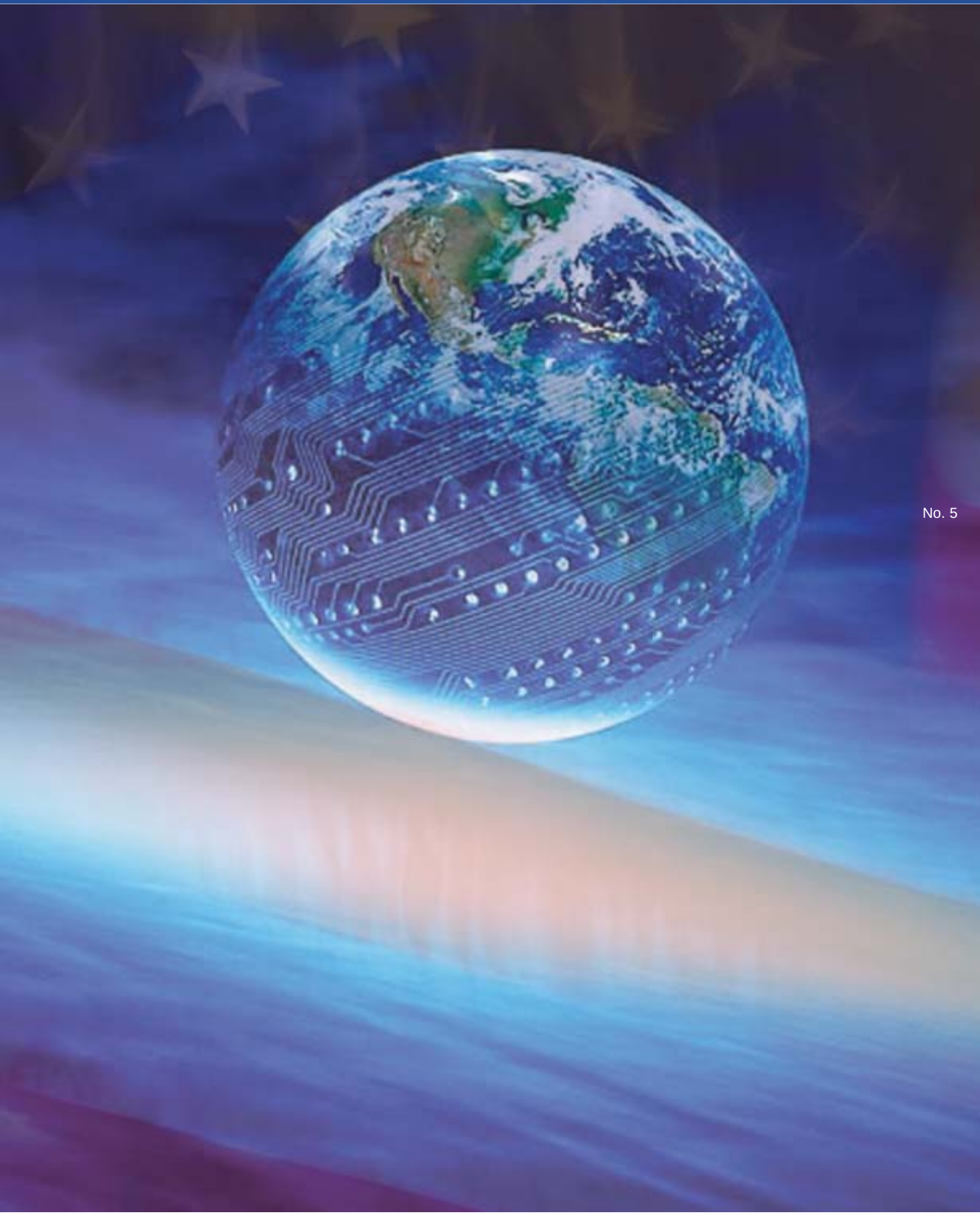
- IA capabilities are dynamic, sufficiently robust, and agile - reconfigurable on demand, available, and consistently controlled at all points of access, with reduced possibility for human and machine error
- Cutting-edge protection, detection, and response technologies are rapidly deployed across all DoD systems and networks, outpacing adversaries' efforts to exploit vulnerabilities

Our Processes

- DoD processes and governance principles meet Netready criteria to support mission accomplishment in a net-centric environment; are continually improved, and are sufficiently dynamic and agile to accommodate rapidly changing needs
- DoD's improved cooperative relationships with academia, industry, and research and development (R&D) organizations allow rapid integration of available technologies and embed enhanced hardware and software assurance solutions in future capabilities

Our People

- IA personnel consistently demonstrate the highest skill levels in managing and deploying the latest technologies and methods
- The entire DoD workforce recognizes the importance of IA, understands its role in it, and is constantly vigilant



No. 5

Protect Information to safeguard data (as information) as it is being created, used, modified, stored, moved, and destroyed, at the client, within the enclave, at the enclave boundary, and within the computing environment, to ensure that all information has a level of trust commensurate with mission needs

The goal of the Global Information Grid (GIG) is to allow information originating from anywhere on the network to be available when required throughout the network. Often the originator has little foreknowledge of who will use this information. Therefore, the new burden on IA is to ensure that all information can be protected from "end to end" and throughout its life cycle.

Data protection must start from the creation of the information, with particular new focus on adding protection levels and access control decisions at that time. Protection must be assured throughout the life cycle of the data: creation, modification, storage, transport, and destruction. We can no longer rely simply on transport mechanisms/link encryption to provide our end-to-end protection. Being part of a global network means that information (e.g., data, metadata) routinely flows in and out of the network through numerous access points. This separation of information from systems requires that the information must be protected, regardless of physical or logical location.

To ensure that information flows protected through the enterprise, an end-to-end IA Architecture must be developed. IA stovepipes and disconnects that prevent the warfighter from accessing needed information must be eliminated. DoD must develop new protection solutions as it initiates Transformational Communications (TC), an effort to transform individual SATCOM systems into a single integrated network accessible to users, regardless of which communications frequencies they currently use. The vision of TC includes Network-Centric Operations, increased capacity and protection, global coverage, flexibility and integrated systems to support a wide spectrum of user needs.

The roles of identity, authenticity, and availability are as important today as confidentiality. DoD has invested in programs such as Public Key Infrastructure (PKI), Biometrics, and Common Access Control (CAC) Cards; however, more effort is needed to ensure that these tools are implemented in a coordinated fashion throughout the Department. Coalition, cross-domain, and collaborative communications require secure labeling and marking ("tagging") of data in order to provide agility for dynamic access control decisions. Our supporting security management infrastructures (i.e., Key Management Infrastructure (KMI), PKI, and network management systems) must manage privileges for a role-based enterprise, support dynamic coalitions, and be easy to use. They must also have a higher level of assurance to protect the vital assets critical to the security of our protection mechanisms. The plug-and-play protection envisioned for the future, to enable devices to be reconfigured for security or functionality purposes without human intervention, must have strong authentication and authorization built in and make use of the transformed Security Management Infrastructure (SMI).

Achieving this goal of trusted data anywhere on the net requires partnerships and combined efforts with other components of the security community (i.e., physical security, personnel security, and critical infrastructure protection) in order to provide an integrated systems security posture.

DoD's strategic objectives for this goal are to:

- Develop and promulgate the GIG IA Architecture
- Develop and implement protection criteria for Net-Centric Operations
- Develop and deploy protection capabilities across the enterprise
- Transform Security Management Infrastructure (SMI) to satisfy the agility demands of the end-state GIG

Strategic Objectives

Develop and promulgate the GIG IA Architecture

Developing the GIG IA Architecture provides the high level plan for information assurance across the enterprise. The results of this plan are increased interoperability, compatible security solutions, and ensured confidentiality, integrity, availability, authentication, and non-repudiation throughout the enterprise.

Performance objectives: To support this strategic objective, DoD will:
- Define the end-to-end GIG IA Architecture
- Ensure the security engineering of all GIG acquisition programs is consistent with the IA Architecture

Develop and implement protection criteria for Net-Centric Operations

Modernized IA policies address the controls necessary to protect information in the defined environment and enable informed risk management decisions. Defining protection requirements, from the data through the network level, enables the appropriate protection standards and criteria to be applied for Net-Centric Operations. Maintaining and revising these policies, standards, and criteria as technology progresses will allow us implement secure solutions.

Performance objectives: To support this strategic objective, DoD will:
- Develop and evolve the IA Policy Framework to satisfy “Netready” needs
- Develop and evolve IA technical standards, criteria, and implementation guides

Develop and deploy protection capabilities across the enterprise

Our protective capabilities must continually evolve in response to the emerging threats and technological advances, to decrease the risk of information loss and operation compromise.

The application of protective mechanisms, integrated with sound system security engineering practices across the enterprise, reduces potential points of failure and provides consistency across multiple access points. This decreases compromises from vulnerabilities, susceptibility to exposure, and complexities for command and control (C2). Of paramount importance is to immediately improve information sharing across the enterprise and with our Allied and Coalition partners and to establish a vigorous end-state plan to achieve multi-level information sharing.

Performance objectives: To support this strategic objective, DoD will:
- Develop, improve, and maintain robust, cutting edge, cryptographic capabilities
- Develop and provide enterprise service for identity and access management and cross domain/communities of interest exchange
- Support and enable multi-level information sharing
- Develop and implement protection control techniques

Transform Security Management Infrastructure (SMI) to satisfy the agility demands of the end-state GIG

We must focus efforts on the Security Management Infrastructure to ensure that it is able to support Net-Centric Operations, protect against cyber threats both internal and external, and minimize impact to operations.

Realizing a robust, usable security infrastructure that can respond on demand to changing technology, capabilities, threats, alliances, and coalitions is key to fighting the Net.

Performance objectives: To support this strategic objective, DoD will:
- Develop and implement robust key generation capabilities
- Provide for assured authentication through implementing and using PKI and Biometrics
- Coordinate the multiple Digital Certificate efforts
- Apply Net-Centric Operations concepts to SMI

Defend Systems and Networks by recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies, ensuring that no access is uncontrolled and all systems and networks are capable of self-defense

DoD systems and networks are constantly under attack and must be continuously defended. To ensure success, defensive mechanisms must be an integral part of the design and implementation of systems and networks across the enterprise. In addition, capabilities must be deployed to react and respond to threats and attacks.

In a collaborative environment, the network requires a significant increase in the autonomous abilities of every "node" and "link" in the system to reduce the propagation of risk. These self-defense mechanisms allow the network to:
- Identify and correct suspicious or unwanted behavior
- Self-heal when penetrated or damaged
- Detect and respond to the differences between legitimate and suspicious demands for system and network resources

The principal points of focus for this goal are the Computer Network Defense (CND) protection, detection, and reaction mechanisms for DoD systems and networks and adaptive configuration management. Adaptive configuration management is a critical capability that includes both active and passive defenses necessary to "correctly" respond to legitimate but changing demands while simultaneously defending against adversary-induced threats.

DoD's strategic objectives for this goal are to:

- Establish GIG Network Defense architecture and to-be baseline roadmap to respond to known and advanced threats
- Develop and enforce CND policies across the enterprise to achieve an optimal readiness posture against the outsider “nation state” attacker as well as the threat posed by the insider
- Evaluate and deploy CND tools and capabilities in a coordinated manner to achieve required operational capability
- Establish mechanisms and procedures within CND response action guidelines that effectively utilize developed CND tools and capabilities to react and respond to events
- Mitigate the Insider Threat across DoD through the implementation of advanced tools, processes, and operational capabilities

Strategic Objectives

Establish GIG Network Defense architecture and to-be baseline roadmap to respond to known and advanced threats

Network and system components must be designed for IA and security and must be capable of being centrally managed and upgraded with new IA/security capabilities. Unfamiliar and complex system and network configurations cannot be adequately defended. Continuing to operate with a patchwork of systems and networks increases the risk of leaving the warfighter exposed to vulnerabilities. Establishing a defensible enterprise network architecture will provide the ability to manage increasing complexity and provide evolving robust responses.

Performance objectives: To support this strategic objective, DoD will:
- Define and establish the baseline GIG Network Defense architecture and validate/harmonize with GIG Architecture
- Develop To-Be architecture

Strategic Objectives

Develop and enforce CND policies across the enterprise to achieve an optimal readiness posture against the outsider “nation state” attacker as well as the threat posed by the insider

In order to mitigate risk and operate DoD networks in an organized and cohesive way, it is important to execute planning, policies and assessments. By laying the framework for operation and administration of network defense, the efforts from this strategic area help the warfighter effectively fight the net by ensuring clear guidance, consistency of operations and high readiness throughout the DoD enterprise.

Performance objectives: To support this strategic objective, DoD will:
- Develop, promulgate, and enforce enterprise CND policies and guidelines
- Integrate exercises, risk assessments and Red/Blue Team assessments and results into operational requirements
- Establish and identify supporting initiatives and assessments

Evaluate and deploy CND tools and capabilities in a coordinated manner to achieve required operational capability

Constant vigilance allows DoD to be ahead of our adversaries and improves our ability to identify emerging threats and impending degradations. Failure to continuously assess and evaluate our systems and networks decreases our ability to detect threats prior to their causing negative effects. By deploying CND tools and capabilities across the DoD enterprise in a coordinated and consistent way, it will mitigate risk of a "weak link" organization and enable desired operational capability on a Departmental level.

Performance objectives: To support this strategic objective, DoD will:
- Deploy standard vulnerability and configuration management tools across the enterprise
- Develop and deploy anomaly detection, threat prediction, and analysis capabilities
- Develop and deploy expanded intrusion detection and data correlation tools and capabilities
- Implement demilitarized zones (DMZs) across the GIG

Establish mechanisms and procedures within CND response action guidelines that effectively utilize developed CND tools and capabilities to react and respond to events

Improved capabilities to react and respond to threats and deficiencies reduce the risk of losing mission-critical capabilities. Vertical and horizontal defensive mechanisms that enable reacting and reporting across the enterprise as well as up chains of command must be developed in order to fully protect our networks. These response action procedures and processes must fit into the CND Response Action Framework in order for rapid and consistent enterprise responses.

Performance objectives: To support this strategic objective, DoD will:
- Create rapid and enhanced forensic support and system administrator capabilities in order to improve incident response across the enterprise
- Identify and develop requirements and initiatives that will lead to enterprise automated threat recognition, reaction, and reconstitution capabilities
- Enable enterprise-wide consequence management [cyber standard operating procedures (SOPs) and continuity of operations planning (COOP)]

Mitigate the Insider Threat across DoD through the implementation of advanced tools, processes, and operational capabilities

DoD realizes the importance of protecting its systems and networks not only from untrusted outsiders, but also from a much more serious threat, the trusted insider. Developing processes and capabilities to mitigate changing threats is a continual process; DoD will be enabled to leverage its other CND initiatives, including policies and tools, to respond and effectively manage threats from its insiders.

Performance objectives: To support this strategic objective, DoD will:
- Conduct a survey of its stakeholders to gather information on current practices, analyze the results and report to appropriate management entities
- Use survey results to deploy a suite of policies, processes, and techniques that will mitigate the threat
- Continuously monitor the enterprise to assure improvement and make necessary adjustments
- Establish Strategic Planning Guidance (SPG) for FY06-12 and develop initiatives to be used in mitigating the Insider Threat across DoD

Provide Integrated IA Situational Awareness/IA Command and Control (C2) integrating the IA posture into a User-Defined Operational Picture (UDOP) synchronized with NETOPS and emerging Joint C2 Common Operating Picture (COP) programs to provide decision makers and network operators at all command levels the tools for conducting IA/CND operations in Net-Centric Warfare (NCW)

The complex and interdependent nature of our information networks and the demands of NCW require shared awareness and understanding across the enterprise to enable effective command and control. Combatant Commanders require sufficient visibility into their network operations including the threats to these networks and the information assurance capabilities applied to protect, defend and respond to them. To meet this need, the IA community must work closely with Combatant Commanders, Services, and Agencies to identify IA Situational Awareness/C2 requirements and build and deploy the capability to fulfill these requirements.

DoD's strategic objectives for this goal are to:

- Develop and deploy an Enterprise Sensor Grid
- Establish effective Indications and Warning (I&W) of potential or ongoing attacks against the enterprise
- Develop and deploy an IA UDOP integrated with evolving NETOPS and Joint C2 COP capabilities
- Conduct near-real-time and integrated IA and Network Operations (NETOPS) decision making across the enterprise
- Harmonize NETOPS, Information Operations (IO), Computer Network Attack (CNA), and Computer Network Defense (CND) policies, doctrine, relationships and operations

Strategic Objectives

Develop and deploy an Enterprise Sensor Grid

Enterprise level information assurance requires the capability to analyze sensor data horizontally and vertically within the entire DoD enclave. The Enterprise Sensor Grid (ESG) will pull information, raw and analyzed, from the CND tools and capabilities deployed in Goal 2 into a cohesive DoD-level system. The ESG will enable information fusion of technical CND data contributing to larger CND Indications & Warning, NETOPS, and IO efforts.

Performance objectives: To support this strategic objective, DoD will:
- Develop policies, processes and procedures for information sharing from enterprise-wide CND sensor capabilities
- Continue the deployment and improvement of the Attack, Sense and Warning (AS&W) capability and other anomaly detection and analysis capabilities for integration into the ESG and supporting enterprise I&W efforts
- Expedite delivery of the ESG to enhance IA support to GIG Bandwidth Expansion

Establish effective Indications and Warning (I&W) of potential or ongoing attacks against the enterprise

Protection of our networks must be a proactive process using all available information on threats to known and suspected vulnerabilities. Threat information ranges from strategic level information on nation-states' and non-state actor' capabilities and intentions to near-real-time tactical information on computer probing activities preparatory to an attack. It includes information from traditional intelligence, counterintelligence and open sources, as well as information from worldwide law enforcement, computer emergency response team (CERT), and government and industry technical sources. Analysis of this information requires the collaboration of intelligence, operations and technical organizations and personnel. Furthermore, as decision cycles are generally extremely short, rapid distribution of this analyzed information is critical to identifying potential threats to the enterprise to warn commanders and enable appropriate defense and response options.

Performance objectives: To support this strategic objective, DoD will:
- Define the process and establish policies and procedures for IA I&W and rapid dissemination of warning information within DoD, and to interagency and international partners
- Integrate relevant and timely Intelligence and Enterprise Sensor Grid data and analysis, and industry, law enforcement, interagency, international military and worldwide CERT information into the IA I&W process

Strategic Objectives

Develop and deploy an IA User-Defined Operational Picture (UDOP) integrated with evolving NETOPS and Joint C2 COP capabilities

NCW demands shared awareness and understanding across the enterprise. A User Defined Operational Picture (UDOP) of the networks, the missions these networks support, and network IA status, provides commanders and network operators with greater flexibility and reduces the risk of negative impacts resulting from unilateral, uncoordinated actions. Interoperability between the IA UDOP and current/emerging common operating pictures at the service, joint, combined and Standing Joint Force Headquarters (SJFHG) levels further enhances the synergy between NETOPS, IA and other military operations.

Performance objectives: To support this strategic objective, DoD will:
- Identify IA/NETOPS information requirements for inclusion in the IA/NETOPS UDOP, including:
  - -Consideration of DoD and Allied/Coalition networks
  - -Input from Interagency, Allied and Coalition partners
- Identify the "As Is" state of IA and NETOPS situational awareness
- Integrate ESG and IA I&W capabilities into the UDOP
- Plan and build the "To Be" or objective IA/NETOPS UDOP ensuring interoperability and synchronization with common operating pictures at the service, joint, combined and Standing Joint Force Headquarters (SJFHG) levels

Conduct near-real-time and integrated IA and Network Operations (NETOPS) decision making across the enterprise

Decision making in isolation often results in unacceptable and unintended consequences. Improved coordination increases our ability to quickly identify, contain, and respond to threats, thereby avoiding the transfer of risks.

Performance objectives: To support this strategic objective, DoD will:
- Provide IA command and control and collaboration capabilities
- Improve, standardize, and integrate CND and Network Operations Center (NOC) operations
- Establish timely IA reporting and notification procedures for the extended enterprise
- Improve the INFOCON process and supporting modeling and simulation capabilities to better develop courses of action, reduce decision and execution timelines, and evaluate effects across the enterprise

Harmonize NETOPS, Information Operations (IO), Computer Network Attack (CNA), and Computer Network Defense (CND) policies, doctrine, relationships and operations

DoD's networks are dispersed, autonomous, overlapping and interdependent entities. Many of these networks are not exclusively owned or controlled by DoD, but may be part of the larger Global Grid, Internet, or Foreign government/military networks. Commanders and network operators must collaborate to ensure the integrity, confidentiality, and reliability of the information for the warfighter. Likewise, CNA and other IO operations, policies and doctrine must be coordinated with IA/NETOPS activities to ensure continuous DoD network operations. Defending our networks requires harmonious relations, cohesive doctrine, and synchronized operations and policies with all organizations that share in their management and protection.

Performance objectives: To support this strategic objective, DoD will:
- Implement proactive CND-Response Actions (CND-RA) policies and capabilities
- Assess and evaluate current and future collaboration efforts and command relationships to identify their operational impacts and coordinate policies and procedures to mitigate risk to DoD networks
- Establish active relationships with other governmental, academic, civilian, international and coalition agencies and organizations to provide critical data interchange
- Evaluate collaboration vulnerabilities and benefits to prioritize DoD efforts and mitigate risk

Transform and Enable IA Capabilities innovatively by discovering emerging technologies, experimentation, and refining the development, delivery and deployment processes to improve cycle time, reduce risk exposure and increase return on investments

The ever-changing and evolving information technology industry stresses DoD's processes and challenges them to keep pace. Maintaining a competitive edge over our adversaries demands that we transform the mechanisms used to develop and deliver new and dynamic capabilities to become more responsive to ever-changing needs. Agility must be a goal that every process meets to maintain this competitive edge. Continuous improvement is mandated. This approach places great importance on harvesting and prioritizing ideas and the rapid development and deployment of concepts and capabilities to enable constant and continuous preparation, shaping, and execution of our responses to the environment.

Net-Centric Operations demand greater process agility and integration. This net-centric environment requires rethinking and innovation in how we reshape the processes of planning, programming, and resourcing in order to rapidly respond to ideas that take root and come to market in time frames faster than current processes can recognize. As such, we must transform how we conduct business among ourselves as well as across traditional boundaries.

Transforming IA capabilities depends heavily on the ability to influence processes the department uses to create, assess, test, and implement new ideas. Developing new approaches to problem solving depends on the synergy between each process as the idea progresses from concept to reality. The focus of this goal is to influence the development of three key processes (Acquisition, Planning, and Innovation) to further the IA mission and support the transformation of the force.

DoD's strategic objectives for this goal are to:

- Ensure that IA is integrated and sustained throughout the lifecycle of all DoD programs
- Improve the quality of strategic decision making and net-centric IA governance
- Expedite the development and delivery of dynamic IA capabilities through innovation
- Enable efficient information sharing and collaboration across traditional boundaries

Strategic Objectives

Ensure that IA is integrated and sustained throughout the lifecycle of all DoD programs

All DoD acquisitions must be accomplished with the idea that security cannot be traded off for added functionality. Stronger controls and increased understanding by Program Managers (PMs) and commanders of the critical capability IA provides for weapons, sensors, and communication systems is needed. Jointness, interoperability, and IA are integral capabilities to any DoD system and full acceptance and implementation of a “Netready” Key Performance Paramater (KPP) is essential. Systems that are designed with these concepts in mind will better meet the needs of the operator without trading functionality. Integrating IA needs into DoD's business processes enables the pervasive and consistent implementation of IA across the enterprise and conforms with the Administration’s “smart buy” concept. We must focus on jointness and program management to ensure that IA is "baked in" and sustained throughout a program's lifecycle.

Performance objectives: To support this strategic objective, DoD will:
- Ensure IA is integrated and defined as “netready” and maintained as a priority within departmental processes (e.g., requirements, acquisition, planning, budgeting and execution)
- Ensure the IA strategy is developed and implemented as a major joint activity
- Fuse vulnerability assessments, lessons learned, exercise results and integrate findings into requirements

Improve the quality of strategic decision making and net-centric IA governance

Realizing the vision requires a concerted effort across the Defense IA Community. To improve the planning function for the IA community we must establish a shared vision with supporting goals, objectives and metrics that will help us prioritize, align and monitor our resources and investments and operations. Only through the cohesive efforts of the IA community can we produce community endorsed priorities to build the business case for the proper funding of much needed IA resources. Prioritizing, aligning and monitoring investments to achieve common goals will improve DoD's overall risk management and return on investment to achieve improved governance of GIG activities.

Performance objectives: To support this strategic objective, DoD will:
- Establish a shared vision, goals, and objectives and implement a standardized strategic planning and management process across the enterprise (C/S/As)
- Develop enterprise-level investment priorities aligned with strategy
- Transform, communicate and implement effective IA governance and guidance
- Establish an enterprise IA performance measurement system at both the local and senior management levels

Expedite the development and delivery of dynamic IA capabilities through innovation

Industry is the primary provider for many IA capabilities and technology is evolving at lightening speed. We need to better position ourselves to take advantage of new, commercially available technologies in real time by establishing relationships with development companies, integrating R&D efforts to better understand where we need to invest in GOTS development, and improving transition time to provide for timely and affordable innovation. We must also improve our internal processes to develop and identify new ideas and concepts, conduct research and development, and deploy cutting-edge capabilities to maintain a competitive advantage. Improving existing processes will result in reducing the rate of obsolescence and costs to sustain legacy capabilities.

Performance objectives: To support this strategic objective, DoD will:
- Increase throughput of ideas for new and dynamic IA capabilities through an improved DoD-IA Industry interface
- Discover and expedite the transition of emerging IA technologies and concepts from non-traditional sources
- Identify, review, test and evaluate technologies against IA needs for experimentation, implementation or investment
- Improve and expand programs and processes fundamental to managing implementation of COTS/GOTS solutions in a risk-managed way

Enable efficient information sharing and collaboration across traditional boundaries

Improved collaboration within the enterprise and with external entities, both internal and external to the U.S. Government, enables us to share the successes and mitigate the results of failures of others as the result of a shared-risk environment. Critical to this sharing is ensuring robust partnerships with other Federal agencies, particularly with the Department of Homeland Security, on areas of common concern. We must create a broader awareness, understanding, and knowledge base from which the IA community can feed. Breaking down cultural and organizational barriers to sharing information and implementing enabling technologies is critical to assuring information in a net-centric environment. Extending the enterprise architecture will result in increased investment efficiency, improved interoperability, reduced technological and skill divergence, and decreased time needed to implement capabilities.

Performance objectives: To support this strategic objective, DoD will:
- Identify and mitigate policy and regulatory impediments to efficient information sharing for Allies, and Coalition partners
- Create mechanisms and define critical partnerships to horizontally fuse information across the enterprise
- Identify and implement secure collaboration tools for the enterprise

Create an IA Empowered Workforce that is well equipped to support the changing demands of the IA/IT enterprise

This Goal is intended to establish an IA professional workforce with the knowledge, skills and abilities to effectively prevent, deter, and respond to threats against DoD information, information systems, and information infrastructures. It is also intended to create the capability to place people with the right skills in the right place at the right time.

This Goal addresses IA awareness, technical training, and security management. IA awareness is targeted to all DoD employees, from entry level to Senior Executive Service (SES) and Flag Officer. Technical training and education focuses on system and network administrators and personnel performing maintenance functions on DoD workstations, systems and networks, as well as IA Officers (IAO), IA Managers (IAM), Designated Approving Authorities (DAA) and their IA staffs.

DoD's strategic objectives for this goal are to:

- Establish baseline certifications across the enterprise
- Provide trained/skilled people when and where needed
- Continuously enhance IA skills to keep current with technology and threats
- Infuse IA awareness and concepts into other disciplines and into other entities

Strategic Objectives

Establish baseline certifications across the enterprise

The Department's current approach to certification is a Component level program. There is wide variation in training content, and the depth and breadth to which topics are addressed. There is inconsistent implementation across the Department, and within Components as well as among military, civilian and contractor workforces. The objective is to define the baseline IA competencies that personnel with various IA responsibilities must possess in order to perform their particular IA functions. Due to the rapid pace of change in technology and associated vulnerabilities and threats, this strategic objective seeks to address standardization of baseline skills by leveraging existing commercial certifications.

Performance objective: To support this strategic objective, DoD will:
• Establish an enterprise-wide IA/IT certification program

Provide trained/skilled people when and where needed

Currently, the Department is not capable of managing its IA/IT workforce effectively or efficiently. There are no existing databases or tools in place to monitor personnel assignments and/or certification status, and billets are not coded for IA/IT. The focus of this objective is twofold: First, to develop appropriate tools, which when populated, will allow Components and Agencies to effectively manage their IA/IT workforce, and second, and the most challenging aspect of this objective, is to identify IA/IT billets and to specify skill indicators for personnel who perform IA/IT functions, regardless of occupational specialty or series, or whether the function is performed on a full or part-time basis. DoD must leverage existing tools, such as specialty pay/bonuses, educational incentive programs and new approaches to foster recruitment and retention. Full acceptance of the IA Scholarship Program (IASP), leveraging the Centers of Academic Excellence (CAEs) and use of visiting IA professors into DoD schools is of paramount importance.

Per***formance objectives:*** To support this strategic objective, DoD will:
• Improve the management of the IA/IT workforce
• Improve the recruitment and retention of IA personnel
• Ensure the effective use of the IASP and CAEs

Continuously enhance IA skill levels to keep current with technology and threats

In light of the dynamic nature of the IT environment, it is critical to maintain and broaden the skills of personnel performing IA/IT functions on a continuous basis. This objective is to provide IA/IT professionals access to the training they need to keep current with tools, techniques, vulnerabilities, threats, policies and key concepts. All methods of training and education need to be leveraged, including community colleges, undergraduate and graduate schools, distributive training, and formal classroom training through Service schools and/or vendors. Reliance on commercial certifications, which require periodic refresher training and/or testing, provides the impetus for IA/IT professionals to get the training they need to maintain current technical skills.

Performance objective: To support this strategic objective, DoD will:
• Improve IA training life cycle management

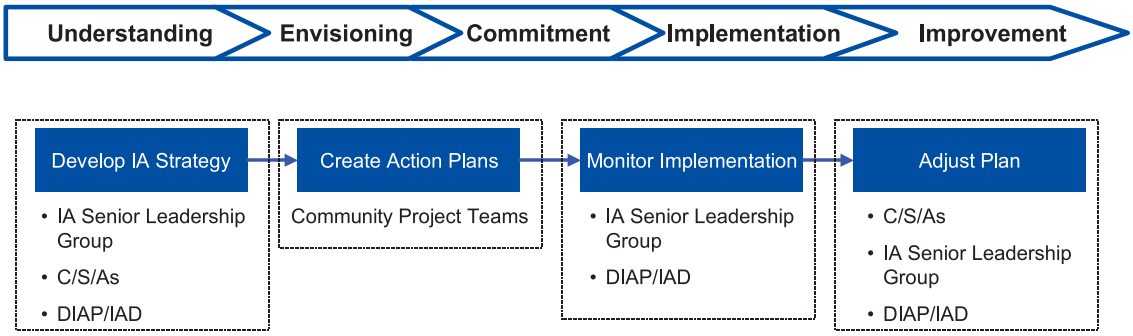
Infuse IA awareness and concepts into other disciplines and into other entities

To increase overall awareness, DoD must identify what other disciplines and external entities need to know about Information Assurance. DoD has the responsibility under PDD 63, to make its distributive products available to the federal workforce and to share best practices, standards, and training tools with academia, industry, Allies and Coalition partners. DoD must provide IA training and awareness content for other disciplines to incorporate into their training and awareness programs. Acquisition, law enforcement, public affairs and legal are examples of such disciplines.

Performance objectives: To support this strategic objective, DoD will:
• Share IA training and awareness products with external entities
• Incorporate IA content into other DoD training program curriculum

This Strategic Plan is the roadmap for DoD in assuring our information, and it serves as a guide for all Services and Agencies within the Department. We will continue to review our vision, goals, and objectives for relevancy, currency, and applicability.

Implementing the IA Strategic Plan requires the involvement of all C/S/As and will require the continued support and commitment of DoD leadership, to include the IA Senior Leadership Group, DoD Chief Information Officer, and the Military Communications and Electronics Board (MCEB). Oversight of the implementation, review, and update of this Strategic Plan will fall to the IA Senior Leadership Group and will generally follow the process outlined below:



The Information Assurance Directorate (IAD) and the Defense-wide Information Assurance Program (DIAP) will serve as the Strategic Management Office for the IA Strategic Plan, and a Goal Lead has been assigned for each of the five IA goals. Successful implementation of the IA Strategic Plan requires the involvement of all Services and Agencies.

If you have questions regarding the IA Strategic Plan, please contact the DIAP via email at **diap@extranet.lotus.com**. Please include the title 'IA Strategic Plan' in the subject of your email.